State of New Jersey
Shared
IT Architecture

February 5, 2003

Contents

General Overview

The State IT community is responsible for the development, maintenance and hosting of several hundred applications serving State agencies, employees, business partners, and citizens throughout the State and the nation.

The State maintains a diverse multi-protocol network, the Garden State Network (GSN), which provides connectivity to all State agencies across New Jersey.

The State has a large technical staff that manages a diverse array of applications on the following platforms:

- IBM 390 mainframe
- Bull mainframe
- MS Windows
- AIX
- Solaris
- LINUX
- Client/Server application platforms

The State is presently aggressively pursuing the delivery of eBusiness services through the Internet and intranets. The focal point for the delivery of most web applications is through the myNewJersey Portal.

eBusiness Technical Architecture Overview

The State has completed the implementation of its eBusiness technical architecture and production environment to facilitate the delivery of web based services to citizens, businesses and employees of the State of New Jersey.

The eBusiness architecture facilitates true portal functionality through the registration and management of intranet, extranet and Internet based members into the myNewJersey Portal.

Management of portal members is role based; i.e., users are assigned one or more roles (e.g., Basic Member, State Employee, Business Owner, etc.), which govern their access to informational and transactional services. Portal members are provided with a myNewJersey homepage which they can customize with available content based on their assigned role(s). (See the section on myNewJersey Portal Management for details.)

The eBusiness architecture provides the following functional services:

- User registration, authentication & security services
- User customizable myNewJersey page creation with role based content channels
- Policy Management
- Directory Services
- ePayment Services
- Enterprise Public Key Infrastructure
- Data, application and web serving platforms

eBusiness Architecture

The eBusiness Architecture is based on Sun Microsystems hardware, SunOne and Oracle software for the J2EE model, and Dell hardware and Microsoft IIS, COM and SQLServer for the Microsoft model. These platforms form a highly robust and scalable environment for the hosting of web based services and are supported in a 7x24 data center in West Trenton, NJ.

Web Serving:

- Sun Microsystems Servers (Solaris) running SunOne Enterprise Server Software
- Dell Servers running MS-IIS

Application Serving:

- Sun Microsystems Servers (Solaris) running SunOne Application Server Software
- Dell Servers running MS-COM
- Custom Enterprise Java Bean ePayment module / VeriSign software libraries

Data Serving:

- The State maintains a variety of database management platforms including Oracle, SQL Server and DB2, and supports legacy IMS, Datacom, Adabas and Honeywell DM4 systems.

Directory Serving:

- SunOne Directory Server (LDAP)

Network Architecture:

- The State maintains a three-tier logical network infrastructure that places web, application and data serving platforms in separate firewall-protected environments. Public (Internet based) access is limited to the web-serving tier only.
- Unless the security requirements for a publicly accessible application are minimal, applications must allow for physically separate web, application and data serving platforms.

myNewJersey Portal Environment:

- SunOne Portal Gateway Servers
- SunOne Portal Servers

Enterprise Public Key Infrastructure:

- Sun Microsystems running VeriSign OnSite (for PKI certificate issuance) and SunOne Enterprise Server Software.
- Dell/Microsoft Windows servers running VeriSign Auto-Authentication software and VeriSign Key Management software for each sub-Certification Authority (i.e., Green, Blue and Orange).

Internet Access and Web Servers

Access to the State's public information is presently provided through the public access Web servers (www.state.nj.us). From there, links are provided to individual agency Web servers. New Jersey currently utilizes one Internet Service Provider (ISP) which is AT&T.

Currently there are a number of production Web servers. One cluster hosts the State's home page and related flat file information (www.state.nj.us). One cluster supports Microsoft IIS web serving, application serving and data serving through SQL Server. One cluster hosts the business logic for Java applications bound for the public web server. A number of applications are already using, and it is expected that future applications will exploit component architecture such as the already developed "ePayment module", an Enterprise Java Bean written in such a way that it can be used for any application that requires the acceptance of a credit card payment.

There are a number of development servers. Some provide staging and development for the Web applications utilizing HTML scripts and graphics bound for the public web server. Others are staging and development servers for Java and Microsoft applications bound for the public Web server.

Application Development Environment and Programming Languages

The application environment for new web based applications is object-oriented design using Java J2EE components running on SunOne application servers. Programs are developed utilizing HTML, Java Server Pages, Java Script, Servlets, Java Beans and Enterprise Java Beans. The goal of the enterprise is to develop reusable components. Authentication and authorization is usually provided by the myNewJersey portal, and leverages pre-defined communities of users and applies role-based policy against those communities.

The Microsoft environment is supported for Commercial Off the Shelf Software but not custom development.

Batch applications are still strongly oriented towards COBOL due to the large pool of trained staff in that area.

Enterprise Application Integration (EAI)

The State has recently evaluated several Enterprise Application Integration (EAI) products and intends to implement a platform in the near future. The selected platform is IBM MQSI. The EAI solution will enable real-time requests from one system to another. This initiative will provide a set of tools that build upon our existing ability to share and manage data.

eForms

The State is currently implementing an enterprise eForms platform based on the Accelio product suite composed of the Adobe Accelio Capture Enterprise Server with the Capture Web module, and the Adobe Accelio Integrate InTempo workflow solution.

This eForms solution will provide forms to New Jersey's external users as well as internal users quickly and efficiently with no download or plug-in. The Capture Web module allows delivery from a single-XML design template, intelligent forms to any browser running on any device, from powerful desktop computers to handheld and wireless devices.

Geographic Information System (GIS) Services

The State has a goal of spatially enabling any application that would benefit from geo-awareness. The State definition of spatially enabled means that the system is:

- capable of integrating spatial data (e.g., data with a location component) with other business data across multiple, heterogeneous data sources; and
- capable of supporting abstract data types (e.g., images, text, and spatial data), spatial operators and functions, and spatial locator indexes.

Managing and accessing spatial data across the State's IT enterprise is facilitated through a gateway which utilizes a combination of technologies including Oracle Spatial and Environmental Research Institute (ESRI) Arc Spatial Data Engine (ArcSDE). Spatial data is served-up in a format that can be accessed by a variety of desktop GIS clients, served out to the Internet using ESRI's ArcIMS technology or by other applications using standard SQL queries. Spatial data is hosted on an Oracle and IBM AIX platform providing for high-availability and scalability.

Internet Map Server (IMS) technology provides the foundation for distributing high-end geographic information systems (GIS) and mapping services via the Internet. This technology also enables users to integrate local data sources with Internet data sources for display, query, and analysis in an easy-to-use Web browser. Our IMS platform is ESRI's Arc Internet Map Server (ArcIMS). ArcIMS is a powerful, scalable, standards-based tool used to quickly design and manage Internet mapping services (web services). IMS technology is currently integrated in the State's Shared Server Infrastructure (SSI) using a three-tier application architecture.

Any proposed solution that includes a GIS component and/or incorporates spatial data is evaluated, planned, designed, and implemented in concert with the OIT Office of GIS. Applications that are geo-enabled are in compliance with the OpenGIS Consortium specifications for spatial data (http://www.opengis.org). The State of New Jersey's preferred GIS software platform is the Environmental Systems Research Institute, Inc.'s (ESRI) set of products and tools (http://www.esri.com).

Data Management Services

The State has built a Logical Data Model and Data Management Framework to manage a core of common data at the enterprise level. This strategy has enabled the State to use relational technologies to collect, disseminate and maintain the integrity of critical data elements across multiple State programs in a manner that is equitable and responsive to all. Adhering to common data standards, State agencies will be able to: collect data once and use it often; warehouse data more effectively for various needs; and better protect the privacy of individuals while improving access to non-restricted information.

Below is a description of the concepts and tools used to accomplish this mission.

Data Warehouse:

- This is a central repository of data that is gathered from a variety of sources.

Data Mart:

- A data mart is a pre-defined selection of data from the warehouse that has been arranged based on the questions that need to be analyzed.

Business Intelligence Tools:

- Query and reporting tools provide rapid development of reports and can be produced by most business people due to a friendly, graphical interface.

Extract, Transform and Load (ETL) Tools:

- ETL tools are use to move and transform thousands of records in a bulk fashion and are designed and administered in a graphical environment. These tools learn about data and systems and enable reuse of knowledge on subsequent projects.

Meta Data Management:

- These tools share definitions of data between each other and the systems that they help to connect. When possible, a common data name and definition is created and shared between systems.

Data Modeling:

- Data modeling tools are used to document, locate and reuse data as well as to describe the relationships between data and systems.

Data Quality Tools:

- These tools are used to analyze data values, find patterns of poor quality, standardize addresses, add geographic coding information to records, and perform sophisticated matching of free-form data to find exact or like matches.

Data Cleansing:

- These tools are used to ensure that data elements are captured and stored in a way to best comply with its business rules and intended application.

Data Integration:

- This tool enables data to be moved 'in bulk' in an intelligent manner, capitalizing on the effort by sharing data among multiple applications.

Data Mining:

- Data mining is a statistical analysis of data for patterns and clusters. These tools can learn from earlier analyses and can look for patterns without guidance.

Supported Database Management Systems (DBMS) Platforms and Knowledge Base

- The strategic relational database for the State is Oracle.
- The State maintains the following RDBMS's: Oracle, DB2 or SQL Server.
- The State maintains the following mainframe legacy databases: IMS, Datacom, Adabas, Bull DM4.
- The State maintains a variety of flat files with a strong emphasis on IBM VSAM for non-DBMS legacy applications.

Data Transfers

The State has implemented two methods of secure file transfer (SFT) to send and receive files utilizing advanced data encryption technologies. The first method is a manual interface through the myNewJersey portal Secure File Transfer Channel. After connecting through an Internet Browser and authenticating to the portal, the user will select the file they need to send, receive or browse and select the source or destination of that file. The transfer will occur using a secure socket layer (SSL) connection and the user will be advised of the success of that transfer. The second method is a client-side Java application that automates the transfer through a host scheduler. This method requires a State-issued NJ State Government Digital Certificate and allows the transfer to occur off-peak without human intervention. Both methods of SFT support 128-bit encryption.

Connect:Direct is used to transfer data over dedicated lines within the Garden State Network (GSN) or to private entities.

Desktop (OIT)

- OIT desktops are Intel based 32 bit platforms using Windows operating systems, a minimum of Windows 95, with present deployments in Windows2000 and XP.
- The standard browser is either Netscape Communicator or MSIE.
- File and print services are typically provided through Novell or Windows 2000.
- Email at OIT is SunOne Messaging and Calendaring. Throughout the state most agencies use MS Exchange, SunOne, Groupwise or Notes.
- There are a variety of client/server applications deployed to desktops, however client/server is no longer a strategic direction for OIT.

Facilities

The State maintains a secure campus for two physical datacenters which process as one logical datacenter connected by high-speed fiber. The State maintains two datacenters on a secure campus in West Trenton and a development staff in an office complex in South Trenton.

Shared Server Infrastructure

The Share Server Infrastructure (SSI) is located at the HUB and River Road Data Centers. It is an area in each computer room where servers are being centralized to offer a common location to manage the distributed environment. Cabinets are provided to “rack” servers and eliminate excess footprint. Implementation of a standard KVM (Keyboard, Video, Mouse) matrix switching backbone solution at both facilities has improved floor space utilization, cable management and server access as well as reduced equipment requirements and power consumption. Optimizing key server resources through common logical and physical environments positions the State to properly plan, manage and control a growing server infrastructure.

Based on the best-supported environments by the IT community, the SSI supports the following operating system platforms:

- Bull GCOS
- IBM OS/390
- IBM AIX
- Sun Solaris
- Windows 2000

Storage Area Network

The State manages two Storage Area Networks (SAN), one at River Road and one at the HUB. A SAN is a network whose primary purpose is the transfer of data between computer systems and storage elements and among storage elements. The SAN consists of a communication infrastructure that provides physical connections, and a management layer which organizes the connections, storage elements and computer systems so that data transfer is secure and robust. The State’s SAN attaches storage devices to servers in a networked fashion, using hubs, switches, bridges, and directors to build the topology. In this case, instead of the normal Ethernet communications network, the SAN is done with fibre (see Appendix 5).

Installing two fibre adapter cards in a server and connecting the server to switches with fibre cables establishes a link to the SAN. Two cards are needed to provide redundant paths to the SAN to eliminate a single point of failure.

Once connected, disk space can be "carved" from the storage array(s) and dedicated to a server. SAN technology presents many benefits to server data storage:

- Centralized storage management
- Easy to add disk capacity dynamically
- Easy to replace a deficient server without lose of data
- Faster response time than internal SCSI disks
- Potential for improved backup and disaster recovery techniques
- Better storage attributes – hardware RAID, dynamic sparing, remote data copy, mirroring and more

Enterprise Systems Management (ESM) Architecture

Enterprise Systems Management (ESM) can be concisely defined as the end-to-end management of the evolving, heterogeneous, multi-platform, distributed computing environment. ESM tools are used to detect, correlate, escalate and prioritize events; manage responses to those events; and report on those incidents in a pro-active, real-time event management environment in order to provide a secure, highly available, robust, multi-platform enterprise infrastructure that meets or exceeds system requirements.

The State has implemented various monitors, distributed storage management, and event management components that are integrated with problem management for the automatic generation of trouble tickets for critical events.

Event management via the Tivoli Enterprise Console (TEC), along with the software products that 'report to it', detect, record, and correlate all enterprise significant events. It is in many ways the central nervous system for our complicated multi-platform computing environment, gathering information on hardware, software and network devices, and, in some cases, curing problems before they actually occur.

Peregrine Systems Service Center (SC) is used for call management, problem management and change management. This product improves client application availability through the automatic notification and escalation of problems via pager and email and the integration of problem and change management.

The integration of the SC with TEC further improves this process by the automatic generation of problem tickets based upon critical events forwarded to the TEC by various monitors (e.g. Netview and Oracle). In some cases problem tickets are generated and the appropriate technical staff notified via email and/or pager before a client is aware of the problem.

The State will also implement Tivoli's Configuration Manager (a robust inventory system), Remote Control, and Monitoring for Transaction Performance (to monitor the performance and availability of eBusiness and enterprise transactions).

Backup and Recovery

The strategic direction of the State is to use Tivoli Systems Management to coordinate, manage and execute backups. Tivoli backup is capable of managing not only a variety of flat files, but the major databases as well through Tivoli and DBMS aware agents.

Performance Assessment Services

Compuware's Network Vantage, LAN and WAN probes are used to perform baseline analysis of the existing network environment prior to deploying new applications. The existing application protocols and their respective volumes traversing the local (LAN) and wide area network (WAN) are identified and their bandwidth consumption, average response times and traffic volumes measured. This analysis can be used as a benchmark comparison against future performance. In instances where a wide area network connection employs Frame Relay technologies, the circuit utilization can be obtained.

Compuware's Application Expert is used to assess applications before they are deployed in a production environment. The results will analyze host/server and network utilization as well as the efficiency and performance of the integrated application functions and will provide response time expectations.

Compuware's Application Vantage and Network Associates "Sniffer Pro" tools are also used to monitor production applications to resolve performance degradations and determine the root cause(s) of poor application performance.

These tools help to determine whether poor application response times are the result of under-powered client workstations, the network infrastructure, the application code or an inefficient host server platform/OS or database.

myNewJersey Portal Management

The myNewJersey Portal environment is provided via a combination of:

- SunOne Portal Server software
- External LDAP directory and Oracle database services
- A custom administration tool, with an HTML user interface, written in Java and served from the eBusiness application server platform

Access to the LDAP directory and Oracle database services is managed by a custom Enterprise Java Bean (EJB) framework served from the eBusiness application server platform.

In the myNewJersey Portal, member services and content management are based on the concepts of User, Role, Entity, Category and Channel.

User:

- Any person, public or private, who is registered with the portal. A person may self-register with the portal, via the Internet, by supplying as little information as a name and email address.

Role:

- A role defines a group of users who share sufficient common interests to warrant the creation of a portal-based user group with access to content and/or transactional systems specifically tailored to those interests.
- Each Portal User is assigned the default role of member. Users may also be assigned one or more additional roles. Roles provide for a centrally managed user environment and each role has a role manager.

Entity:

- Groups of users who share a common organizational interest belong to the same entity. Each time a user is assigned a role, that user/role is associated with an entity. Entities allow for decentralized user management as there is always a manager for each entity in the portal.

Category:

- A grouping of roles into a broad service delivery category. Examples may include the Government, Business or Employee category.

Channel:

- A content provider designed to be delivered through the myNewJersey portal page. Channels are associated with one or more roles.

Public Key Infrastructure

The State has implemented and is hosting a private certificate authority using products and services from VeriSign to implement an enterprise Public Key Infrastructure.

OIT technical staff have implemented the following components for enterprise PKI:

- Registration
- Certificate Issuance
- Revocation of Certificates
- Storing and Retrieving Certificates
- Certificate Revocation Lists
- Key Lifecycle Management

The Enterprise Certification Authority Model will include State of New Jersey Green, Blue and Orange certificates denoting increasing levels of trust/registration requirements.

This infrastructure is expected to meet the majority of PKI business requirements for Internet, Intranet and Extranet users. A distributed administration model will give agencies control over registration and issuance of certificates. OIT will maintain the Certificate Revocation function, Certificate Revocation Lists, and Key Lifecycle management. A statewide Certificate Policy and Certification Practices Statement will govern certificate issuance.

Security requirements for the myNewJersey Portal environment will vary, ranging from simple user name and password to more stringent requirements including the use of PKI.

Enterprise Directory Services

The State maintains a Lightweight Directory Access Protocol (LDAP) compliant enterprise directory service for all State employees (NJ Direct). It is currently in use supporting PKI deployments as well as agency-based extranet user management. The directory is based on Sun ONE Directory Server Software. State personnel names, locations, telephone system data, and e-mail addresses have been integrated into the directory. Approximately 80,000 entries, one for each State employee, now reside in the directory.

Synchronization with other State agency directories is accomplished through data feeds. The State is currently piloting a meta-directory effort to automate the synchronization process. In the future, the enterprise directory will provide directory services for county and municipal employees as well as citizens and businesses.

The myNewJersey Portal Environment uses a combination of LDAP directory services, an Oracle based datastore and NJ Direct to store user authentication, demographic and role assignment data.

Network

State of NJ Three-Tier Network Architecture

The State of NJ has implemented a three-tier network architecture to provide state-of-the-art security design to the State’s core Garden State Network resources. This architecture consists of three firewalls protecting our core network from the Internet world (i.e., a ‘double DMZ’ model). See attached diagram of eBusiness Technical Architecture.

According to our security policy, an Internet user can only communicate with servers on the public tier. A public tier server can only communicate with a secure tier server, and only a secure tier server can communicate with core network. A server or workstation can communicate with any device on a higher layer, and the response can come back to only that originating device.

Therefore, in communicating downward in the model from the Internet, at each tier there must be a process, which takes a request and hands it down to the next layer. Typically, this model fits well with distributed application design, where tier 1 handles presentation, tier 2 handles business logic, and tier 3 houses the data. (Web servers, Application servers, and Data servers.)

In some instances, two tier applications are accommodated in this model by placing the data on the second tier. The practice of placing all components on the first tier (one-tier applications) is no longer acceptable.

Tunneling, simple pass-through proxy, ‘double tier hops’, and other techniques that do not apply policy or process to an inward bound communication at each tier, are not allowed. To do so would compromise the integrity of all remaining applications that do follow the security policy.

Network Protocols

The State uses the TCP/IP family of protocols as the standard network protocol to ensure technical compatibility and efficient use of the available data transport resources. Other protocols are in use, but their use is being phased out in favor of TCP/IP.

Garden State Network Architecture

The Office of Information Technology builds and manages a multi-agency, multi-protocol network (Garden State Network, GSN) across New Jersey. This network supports State agencies through dedicated and switched services in support of centralized and distributed data processing applications resident in mainframe, mini-computer, local area network (LAN), and personal computer environments. The GSN also provides Internet and email services. The GSN's reach, features and capacities are constantly being expanded to meet these needs.

The GSN is comprised of six main node facilities. These nodes are interconnected to form the statewide backbone network. The backbone is designed with multiple paths to increase service reliability and availability in the event of a failure (see Appendix 4 – Garden State Network). Primary transport technologies in use include frame relay, Integrated Services Digital Network (ISDN), Asynchronous Transfer Mode (ATM), T-1, T-3, OC3, OC12 and SONET. The major contracted carrier service providers at this time are AT&T and Verizon. The individual agency locations connect to their central node primarily with T-1 ATM, frame relay, or point-to-point services. The Inter-LATA circuits connect the main nodes via T-3 and OC3 technologies.

The GSN currently serves over 45,000 IP addressable devices. Included in this device count are over 1000 routers, and over 1000 application servers. Individual agencies administer their own local infrastructures.

The State employs Domain Naming Service (DNS) for enterprise wide name resolution. An initiative to convert to Dynamic Domain Naming Service (DDNS) is currently in the planning phase.

For Internet connectivity, New Jersey currently utilizes two 45 mbps Point-to-Point circuits with gigabit switched segments to ISP - AT&T. The two circuits are located in SAC (State Police Systems and Communications Center) and the HUB in West Trenton. They connect into different AT&T Service Node Routing Complexes (SNRCs) located in Washington, D.C. and Philadelphia, Pennsylvania.

Internet access to the State's public information is provided through the public access Web server (www.state.nj.us). From there, links are provided to individual agency Web servers. There are also a number of public web servers hosting a variety of government related applications.

The principle consolidation point for government information, applications and services is through the myNJ Portal which acts as an authentication and authorization point, can broker services, and provide customization and personalization to a variety of user communities.

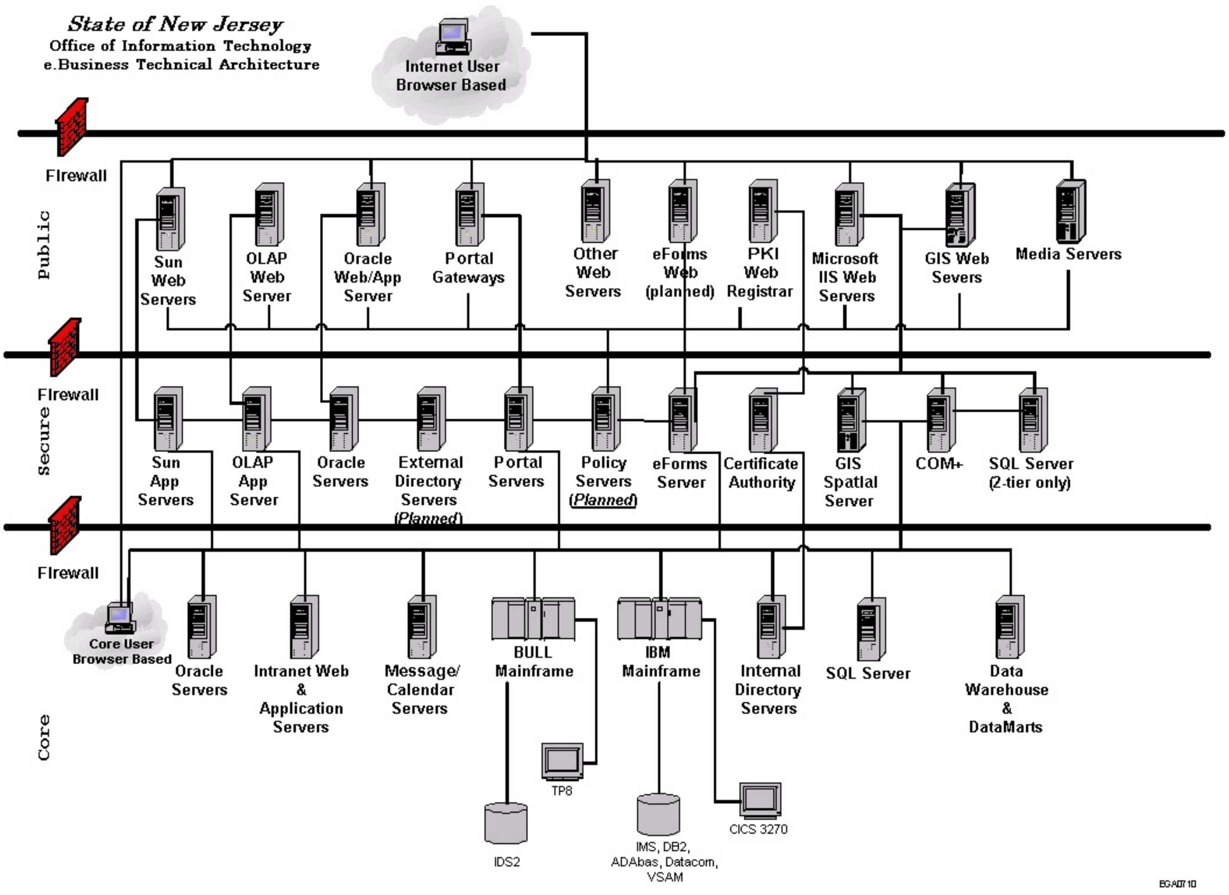
Currently there exists one entry and one exit point between the GSN and the Internet, that being through a firewall which uses IP protocol. Additional firewalls have been implemented to separate the three tiers. The GSN firewall infrastructure provides a physical 3-tier architecture designed as follows: Tier 1 for web serving, Tier 2 for application serving (business logic), and Tier 3 for a variety of core services including databases. The firewalls have been configured such that a higher secure host (i.e. core) can initiate a connection to a less secure host (i.e., secure or public) but a less secure host cannot initiate a connection to a higher secure area without a proper firewall rule. The policy prohibits advancing inbound more than one tier at a time without a process to supervise communications with the next tier. Firewall rules are created to allow specific connection defined by specific ports. The typical public access is by port 80 (http) and 443 (https).

Dialup services are provided to limited users through Cisco 5200's. It provides 56K asynchronous capabilities for remote access.

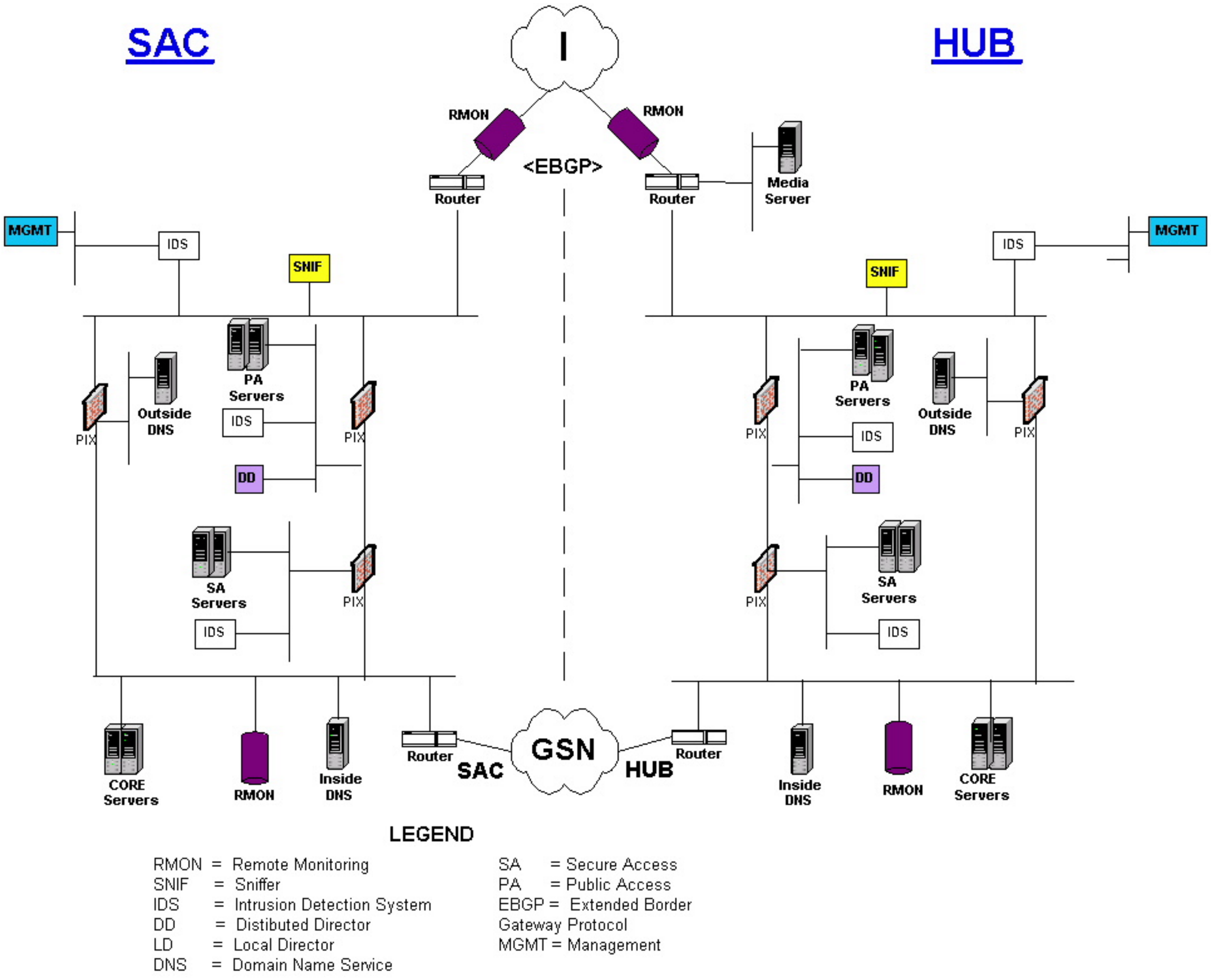
Extranet connections require point-to-point connections from the vendor to the secure layer of the firewall infrastructure. The cost of these connections varies based on the circuit ordered.

Unsolicited inbound file transfers (FTPs) to the State are not allowed. FTP is only allowed within core or as a 'pull' back to core. (See section on Data Transfers for details.)

Appendix 1 - Logical Network Diagram



Appendix 2 - Physical Network Diagram



Appendix 3 - Products and Technologies

Category	Product	Direction *
Operating Systems		
	AIX	P
	GCOS8 (Bull)	S
	LINUX	A
	OS390	A
	Solaris	P
	Windows 2000	A
	Windows NT	S
	Z/OS	A
Database Platforms		
	Adabas	S
	Datacom	S
	DB2	A
	IDS2	S
	IMS	S
	Oracle	P
	SQLServer	A
	VSAM	S
Transaction Management		
	CICS	A
	TP8 (Bull)	S
Languages		
	COBOL	A
	J2EE Java	P
	Natural	S
	Perl	A
	HTML	P
	JavaScript	A
	SQL	P
	Visual Basic	S
	.ASP	A
	Oracle Forms/Rpts	A
	XML	P
Portal Services		
	Sun ONE Portal Server	P
Directory Services		
	Active Directory	A
	Sun ONE LDAP	P
Data Transfer		
	Secure File Transfer	P
	Connect:Direct	A

Legacy Data Access		
	CICS Transaction Gateway	A
	Entire X	A
EAI (Enterprise Application Integration)		
	IBM WebSphere MQSI	P
eForms		
	Adobe Accelio Capture Enterprise Server w/Capture Web module	P
	Adobe Accelio Integrate InTempo workflow solution	P
GIS Technology		
	ESRI: ArcSDE/Oracle Spatial – Spatial Data Hosting	P
	ArcIMS/ArcMap Server – Internet Map Server	P
	RouteServer – Routing and Driving Directions	P
	Metadata Server – Spatial Data Catalog	P
Application Servers		
	Oracle	A
	Sun ONE	P
Web Servers		
	IIS	A
	Sun ONE	P
	Oracle	A
Messaging Technology		
	IBM MQ Series	P
Application Developer Desktop		
	Windows 2000	P
	Windows 98	S
	Windows 95	S
	Windows NT4	S
Security Tools		
	ACF2	A
	VeriSign PKI	A
	SSL	A
Network Management		
	Tivoli Suite	P
Imaging		
	FileNet	A
Mail		
	Sun ONE (OIT), also integrate to Exchange, Notes, GroupWise	Not Rated
Calendar		
	Sun ONE (OIT), also integrate to Exchange, Notes, GroupWise	Not Rated

Audio / Video

Real Media	A
Microsoft	A
Avid Xpress	A

OLAP (Online Analytical Processing)

Business Objects	P

Software Administration

SourceSafe	A
CVS	P
CA Librarian	A

Data Management Tools

DataStage (ETL Platform)	P
Integrity (Data Quality Platform)	P
MetaStage (Meta Data Repository)	P
PowerDesigner (Data and Process Modeling)	A
Oracle Designer (Data Modeling)	A

Data Mining & Statistical Analysis

SAS	P

Reporting Tools

Oracle Reports	A
Crystal Reports	A
Business Objects	P
Focus	S
Magna8	S

Development Tools

Macromedia DreamWeaver (HTML)	A
Forte	P
Adobe	A
Quark	A
Macromedia Flash	A
Macromedia Fireworks	A
Pagemaker	A

Print Services

IBM Advanced Function Printing	P

* Direction Key:

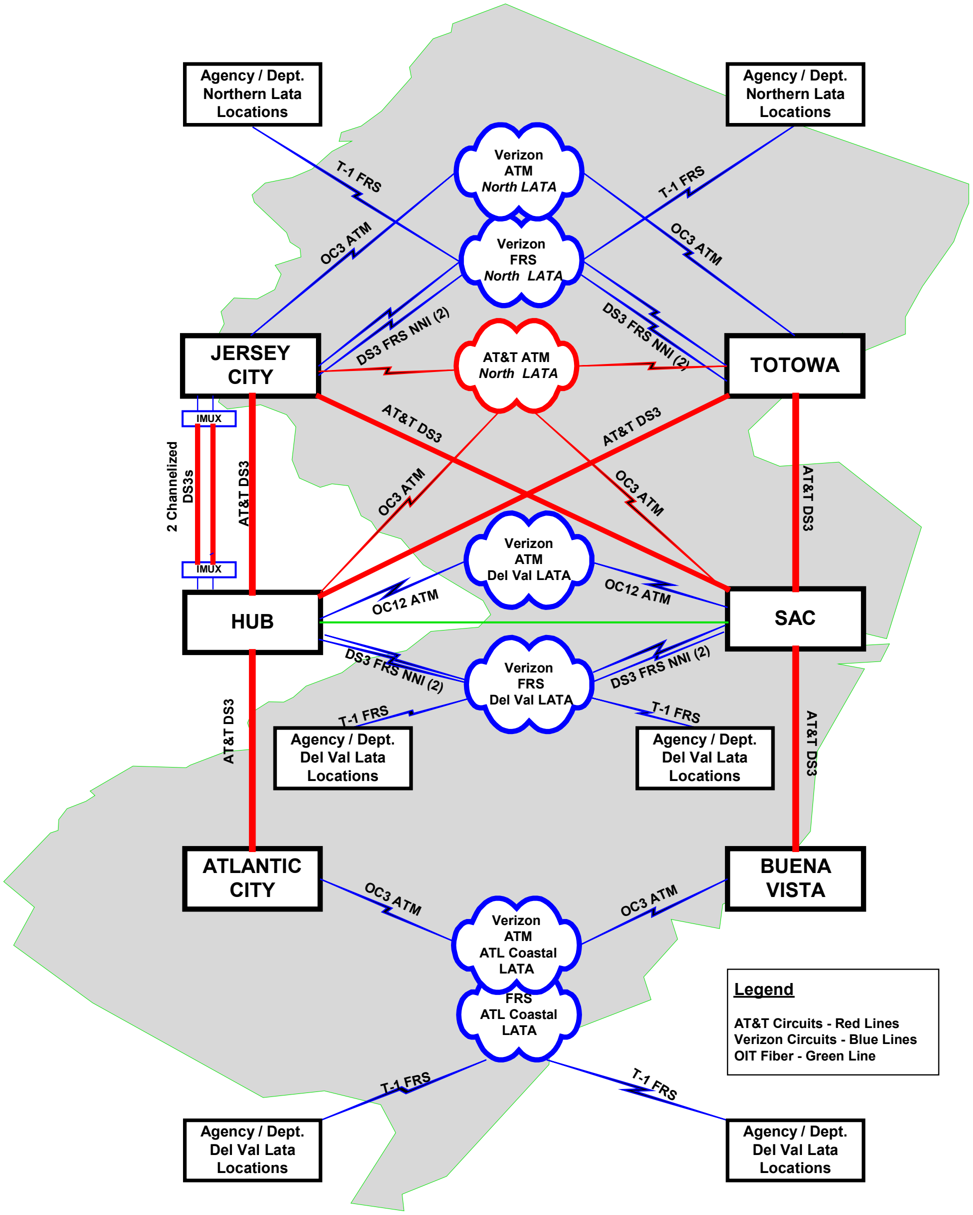
P = Preferred
This represents our strategic direction.
The State will give priority to this technology.

A = Acceptable
This represents our minimum requirements.
The State considers this technology adequate/satisfactory.

S = Sunset
The State deems this technology undesirable/unacceptable.

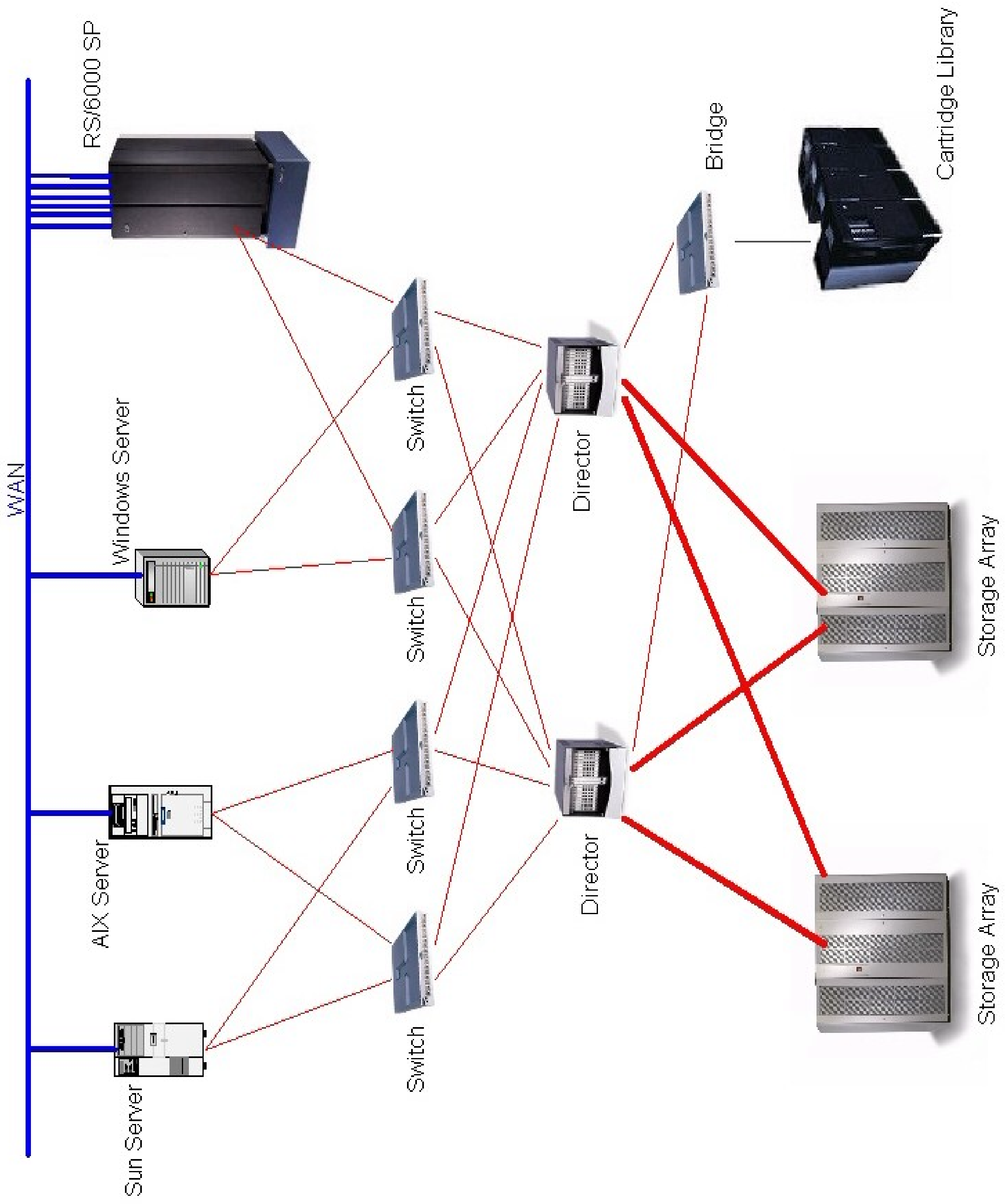
Appendix 4 – Garden State Network

Garden State Network
GSN August 2002



Garden State Network Layout Figure 1

Appendix 5 – Storage Area Network (OIT)


WAN
Sun Server
AIX Server
Windows Server
RS/6000 SP
Switch
Switch
Switch
Switch
Director
Director
Bridge
Storage Array
Storage Array
Cartridge Library